Лекция 2

Методы идентификации и аутентификации

Часть 2

Методы опознавания и подтверждения подлинности

в компьютерных системах

Определения

Идентификация в информационных системах — присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов.

Аутентификация в информационных системах - это проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).

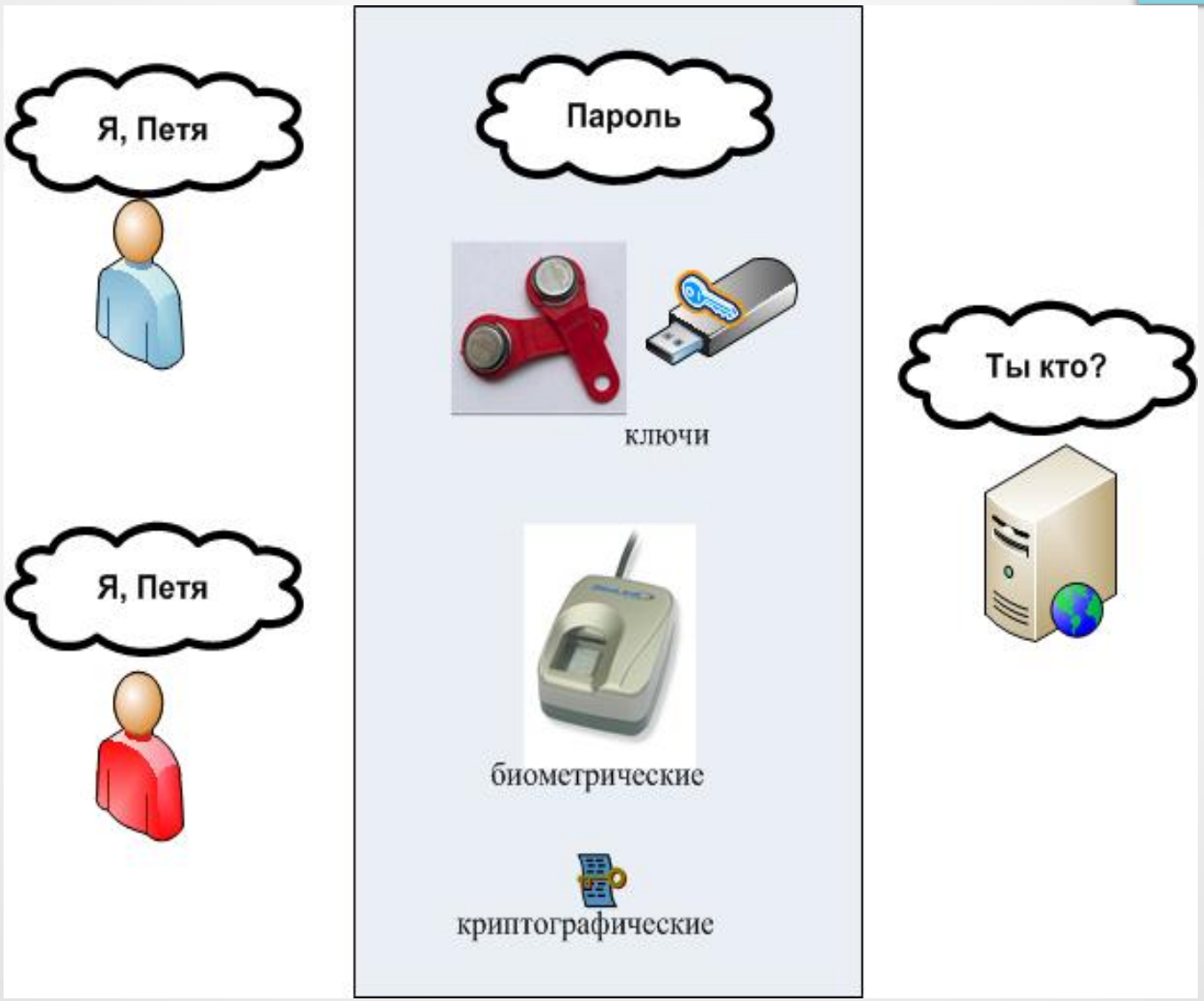
Авторизация - процедура предоставления субъекту определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к её ресурсам.

Администрирование - процесс управления доступом субъектов к ресурсам системы. Данный процесс включает в себя:

- создание идентификатора субъекта (создание учётной записи пользователя) в системе;
- управление данными субъекта, используемыми для его аутентификации (смена пароля, издание сертификата и т. п.);
- управление правами доступа субъекта к ресурсам системы.

Аудит - процесс контроля (мониторинга) доступа субъектов к ресурсам системы, включающий протоколирование действий субъектов при их работе с ресурсами системы в целях обеспечения возможности обнаружения несанкционированных действий.

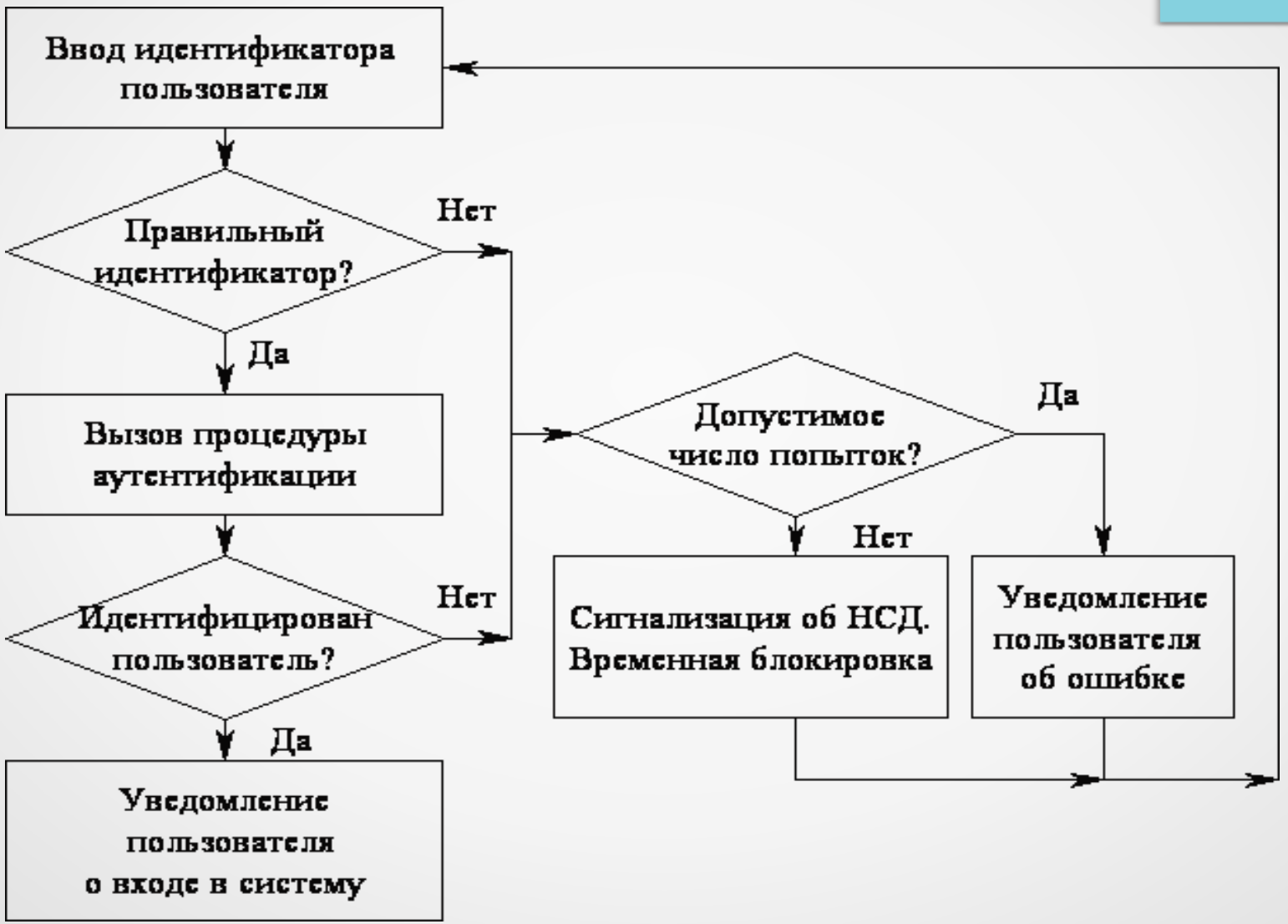
Подтверждение подлинности



Подтверждение подлинности

Выбор технологии аутентификации

Процедура «идентификации»



«Простой пароль»

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на паролях – секретных идентификаторах субъектов. Здесь при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам АС.

«Простой пароль»

Плюсы и

Минусы:

- подбор паролей
- просмотр паролей в системе
- перехват паролей при передачи
- пароль можно «подсмотреть» при вводе
- человеческий фактор – человек не может запомнить сложные пароли (записывает), диктует открытым способом (по телефону) и т.д.
- каждый раз нужно набирать на клавиатуре
- нужна предварительная регистрация пользователя в системе

Модификации схемы «Простой пароль»

1. Простейшие методы модификации схемы простых паролей.

   В этом случае пользователю выдается список паролей («длинный пароль»). При аутентификации система запрашивает у пользователя пароль, номер в списке которого определен по случайному закону. Длина и порядковый номер начального символа пароля тоже могут задаваться случайным образом.

2. Ограничение времени (или задержка) и числа попыток ввода пароля.

3. Методы «запрос-ответ»;

   При использовании метода «запрос-ответ» система задает пользователю некоторые вопросы общего характера, правильные ответы на которые известны только конкретному пользователю.

Модификации схемы «Простой пароль»

4. Функциональные методы.

Функциональные методы основаны на использовании специальной функции парольного преобразования . Это позволяет обеспечить возможность изменения (по некоторой формуле) паролей пользователя во времени

Идея метода функционального преобразования состоит в периодическом изменении самой функции . Последнее достигается наличием в функциональном выражении динамически меняющихся параметров, например, функции от некоторой даты и времени.

Пользователю сообщается исходный пароль, собственно функция и периодичность смены пароля.

Нетрудно видеть, что паролями пользователя на заданных - периодах времени будут следующие: x, f(x), f(f(x)), ..., f(....f(x)...).

- исходный пароль - слово или число X, например число 31;
- функция F(X), например, Y= (X mod100) • D+ W, где (X mod100) - операция взятия остатка от целочисленного деления X на 100, D - текущий номер дня недели, а W - текущий номер недели в текущем месяце;
- периодичность смены пароля, например каждый день, каждые три дня или каждую неделю.

Модификации схемы «Простой пароль»

5. Метод «рукопожатия»

Метод состоит в следующем: функция парольного преобразования известна только пользователю и системе защиты.

При входе в АС подсистема аутентификации генерирует случайную последовательность *x*, которая передается пользователю.

Пользователь вычисляет результат функции $y=f(x)$ и возвращает его в систему.

Система сравнивает собственный вычисленный результат с полученным от пользователя.

При совпадении указанных результатов подлинность пользователя считается доказанной.

Достоинством метода является то, что передача какой-либо информации, которой может воспользоваться злоумышленник, здесь сведена к минимуму.

Модификации схемы «Простой пароль»

6. Ограничение срока жизни пароля

7. Методы, использующие одноразовые (динамично изменяющиеся) пароли

- Сложность реализации.
- Проблемы синхронизации списков паролей.
- Перехват - методы аутентификации, основанные на одноразовых паролях, также не обеспечивают абсолютной защиты. Например, если злоумышленник имеет возможность подключения к сети и перехватывать передаваемые пакеты, то он может посылать последние как собственные.

Модификации схемы «Простой пароль»

8. Шифрование списков паролей в АС.

- Симметричные криптоалгоритмы
- Несимметричные криптоалгоритмы
- Однонаправленные функции (необратимые преобразования)

Модификации схемы «Простой пароль»

9. Запоминаемость паролей (слабые методы)

- Названия домена вперемежку с логином («gooUSERglcom», «UmailruSer»);
- Определенная стандартная фраза, которая прикрепляется к домену («passgoogleru», «passhabrahabrru»);
- Распространенное слово вперемежку со значащими цифрами и другими знаками («321DR67ag0On», где 32167 – чит, который вызывал 5 черных драконов в Heroes of Might & Magic);
- Русские слова в английской раскладке («,k.lj [htyf» — «блюдо хрена»);
- Перестановка букв («Мойна и Вир», «twirret»);

Модификации схемы «Простой пароль»

Запоминаемость паролей (сильные методы)

- Произносимость
- Используйте в пароле антонимы, синонимы и омонимы и др. в различных комбинациях со знаками препинания и цифрами («молодойстарик18лет», «svetlo! темный», «собака=@»);
- Используйте формулы и выражения («12!=12.1», «@die(‘hard’)», «echo $string»);
- Используйте ненастоящие адреса электронной почты («Ya.Krevedko@ya.ya»);
- Используйте рифмы в пароле («google’shmugl», «HABRa_kadabra»);
- Повторение («http://http://double_pass», «zloe_zlo»);
- Визуализация («Зомби выели мне мо3г», «КуКла.Даша.плачет»);
- Преувеличение («25 часов утра», «Путин’а в мэры!», «почеши МНЕ желудок»);
- Используйте мат в паролях (тут упражняйтесь сами);

Модификации схемы «Простой пароль»

10. Генерирование паролей
    - Повышение степени не тривиальности пароля
        - Отсутствие словарных слов и частей распространенных паролей в составе пароля;
        - Отсутствие шаблонов при составлении пароля (под шаблоном понимается логический алгоритм генерации пароля, например: «Med777ведев», «12@йцу@21» или даже «q1w2e3r4t5»);
        - Стохастические последовательности символов из различных групп (строчные, прописные, цифры, знаки препинания и спецсимволы);
    - Ограничение длины пароля
    - Затруднение словарного подбора
    - Генераторы случайных чисел

Методы взлома парольной защиты

Подбор пароля

Вероятность подбора пароля уменьшается также при увеличении его длины и времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля. Ожидаемое время раскрытия пароля *T* (в днях) можно вычислить на основе следующей приближенной формулы:

$$T = (A\ S)\ t / 2$$

Здесь:

A - число символов в алфавите, используемом для набора - символов пароля;

S - длина пароля в символах, включая пробелы и другие служебные символы;

t - время ввода пароля в секундах с учетом времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля.

Например, если *A*=26 символов (учтены только буквы английского алфавита), *t*= 2 секунды, а *S*= 6 символов, то ожидаемое время раскрытия *T* приблизительно равно одному году.

Методы взлома парольной защиты

- Метод логического угадывания. Работает в системах с большим количеством пользователей. Злоумышленник пытается понять вашу логику при составлении пароля (логин+2 символа, логин наоборот, самые распространенные пароли и т.п.) и применяет эту логику ко всем пользователям. Если пользователей много, очень скоро произойдет коллизия и пароль будет угадан;
- Перебор по словарю. Этот вид атаки применяется, когда база данных с хешированными паролями слита с сервера. Может сочетаться с заменой букв (опечатки) или с подстановкой цифр/слов в начало или конец слова в качестве приставки или суффикса. Также используются словари, набранные в неверной раскладке клавиатуры (русские слова в английской раскладке);
- Перебор по таблице хешированных паролей. Передовой метод взлома паролей, когда хеши уже сгенерированы и остается только найти в базе соответствие хеша паролю. Работает очень быстро даже на слабых машинах и не оставляет никаких шансов владельцам коротких паролей.
- Другие методы: социотехника и социальный инжиниринг, использование keylogger'ов, снифферов, троянов, термоанальный и т.п.

Методы взлома парольной защиты

- Самая распространенная цифра в паролях – 1, встречается в 21% паролей, в то время как остальные цифры присутствуют в 7%-10% случаев;
- 24% всех паролей состоят из 6 символов;
- Более 60% всех паролей содержат только строчные символы;
- Самый распространенный пароль в сети: «123456»;
- Существуют программы, способные проверять более миллиона паролей в секунду на процессоре Pentium 4 с частотой 3ГГц;

Аутентификация с помощью аппаратных средств

Аутентификация с помощью аппаратных средств

- ГЕНЕРАТОРЫ ОДНОРАЗОВЫХ ПАРОЛЕЙ
- СМАРТ КАРТЫ

- USB-КЛЮЧИ

- ГИБРИДНЫЕ УСТРОЙСТВА

Аутентификация с помощью аппаратных средств

Компания	Продукт	Функции
Рускард	"Мастер паролей". Комплекс имеет сертификат ГТК России на работу с конфиденциальной информацией. Заканчиваются работы по сертификации продукта в системе сертификации ГТК и МО РФ на предмет допуска к государственной тайне	Идентификация пользователей и разграничение прав доступа к сетевым и терминальным ресурсам. Использует технологию смарт-карт и принципы парольной защиты информации
ОКБ САПР	"Шипка"	Электронный документооборот с использованием ЭЦП. Реализован под USB- разъем, включает коды аутентификации, электронно-цифровую подпись, электронный ключ, систему управления ключами, ключи для защиты программ и данных
ОКБ САПР	СЗИ "Аккорд"	Реализует коды аутентификации на контроллере, результат хэш-функций, ключи шифрования
Крипто-Про	Средство криптографической защиты информации "Крипто-Про CSP" разработано в соответствии с крип-тографическим интерфейсом фирмы "Микрософт". Сертифицировано ФАПСИ по уровню "КС- 1 " и "КС-2"	Проведение формирования и ввода секретных ключей и ЭЦП с помощью следующих типов носителей: дискета; процессорные карты MPCOS-EMV и российские интеллектуальные карты (РИК); таблетки Touch-Memory; USB-ключ e Token
Актив и Анкад	USB-ключ ruToken	Реализация защиты целостности с помощью ЭЦП и безопасное хранение паролей, ключей и цифровых сертификатов
MultiSoft	MAGICSECURE3100	Обеспечение аутентификации с помощью устройства контроля доступа по отпечатку пальца на мыши
MultiSoft	CRYPTO IDENTITY	Реализация идентификации и аутентификации с помощью USB-устройства. Использует нестандартную для России криптографию RSA, а также механизмы паролей, хранения ключей
НПП "ФАКТОР-ТС".	Сетевые решения "ДИОНИС"	Идентификация и аутентификация сетевого трафика, электронной почты и файловых транзакций

Аутентификация с помощью аппаратных средств

Компания	Продукт	Функции
СИГНАЛ-КОМ	Сведения не предоставлены	Идентификация и аутентификация в защищенном документообороте с помощью библиотеки криптографических преобразований "Message-PRO" и "Data-PRO", "IP Safe-PRO" (IPsec)
ИНФОРМЗАЩИТА	АПК"Континент-К"	Реализация сервиса сетевой защиты, включая идентификацию и аутентификацию
ИНФОРМЗАЩИТА	Электронный замок "Соболь"	Реализация идентификации и аутентификации при доступе к персональному компьютеру
ИНФОТЕКС	flAKViPNet	Построение комплексных VPN
Aladdin Software Security R.D.		Смарт-карты и электронные ключи e Token - средство аутентификации, хранения ключей шифрования, ЭЦП, паролей Аутентификация с помощью USB-ключей и смарт-карт eToken, обладающих защищенной PIN-кодом памятью. Генерация ключей шифрования с помощью собственного встроенного в устройство микропроцессора
ОАО "Ангстрем" и ОАО "Российская электроника"	Сведения не представлены	Идентификация и аутентификация с помощью смарт-карт в интегрированных приложениях
ОАО "ЭЛВИС-ПЛЮС"	Сведения не представлены	Идентификация и аутентификация пользователей и VPN
АОЗТ "Инфосистемы Джет"	Сведения не представлены	Идентификация и аутентификация в сети

Протоколы аутентификации в сети

PAP (Password Authentication Protocol) - двусторонний протокол обмена подтверждениями, предназначенный для использования с протоколом PPP. PAP является обычным текстовым паролем, используемым в более ранних системах SLIP.

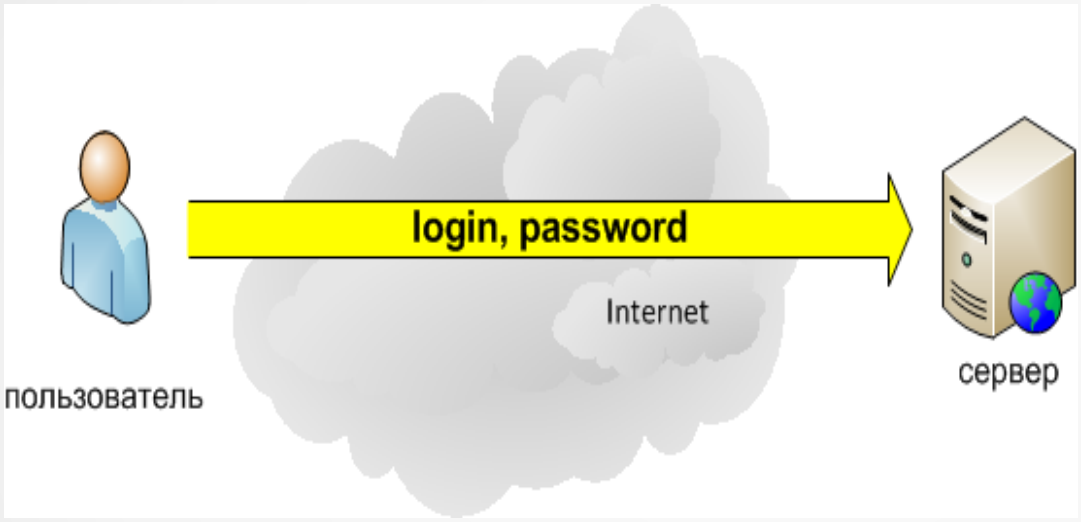
CHAP (Challenge Handshake Authentication Protocol) - это трехсторонний протокол обмена подтверждениями, предполагающий лучшую защиту, чем протокол аутентификации PAP (Password Authentication Protocol).

MS-CHAP (MD4) Использует версию Microsoft протокола.

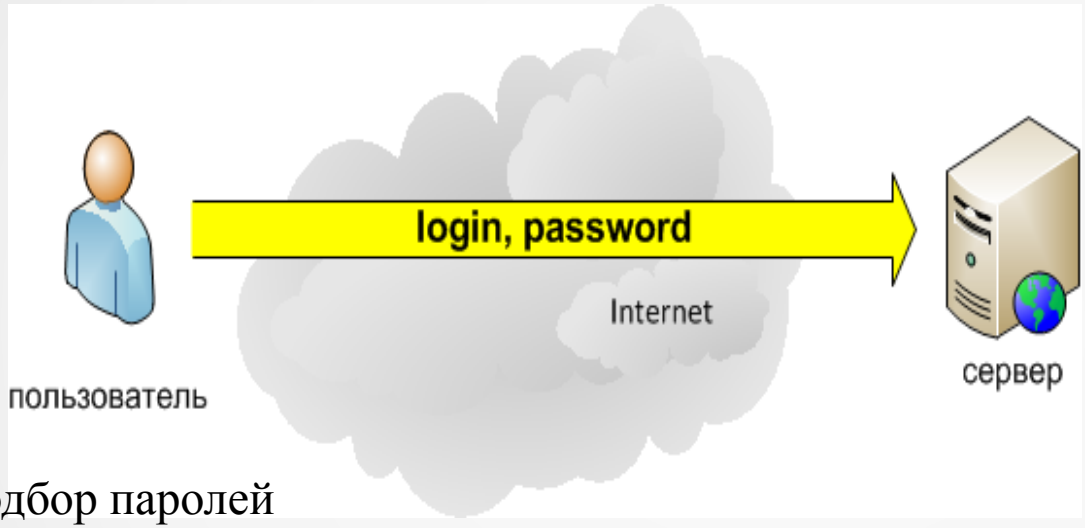
MS-CHAP-V2 Предоставляет дополнительную возможность для изменения пароля, недоступную с MS-CHAP-V1 или стандартной аутентификацией CHAP.

EAP (Extensible Authentication Protocol) представляет собой расширяемый механизм аутентификации, позволяющий унифицировать процесс проверки подлинности пользователей, предоставляя при этом участникам соединения возможность использования самых разнообразных схем аутентификации.

Удаленная аутентификация PAP

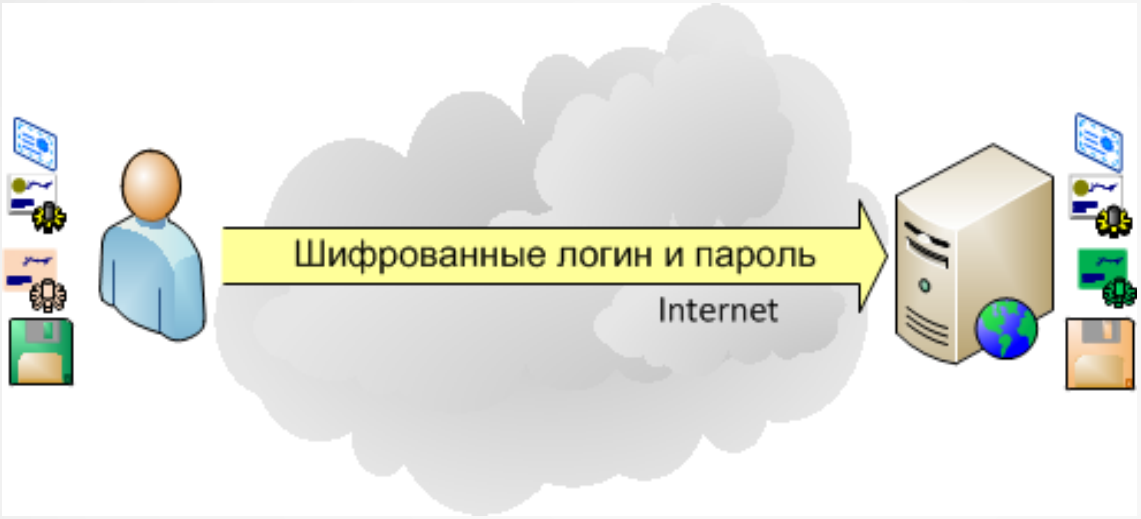


Удаленная аутентификация PAP



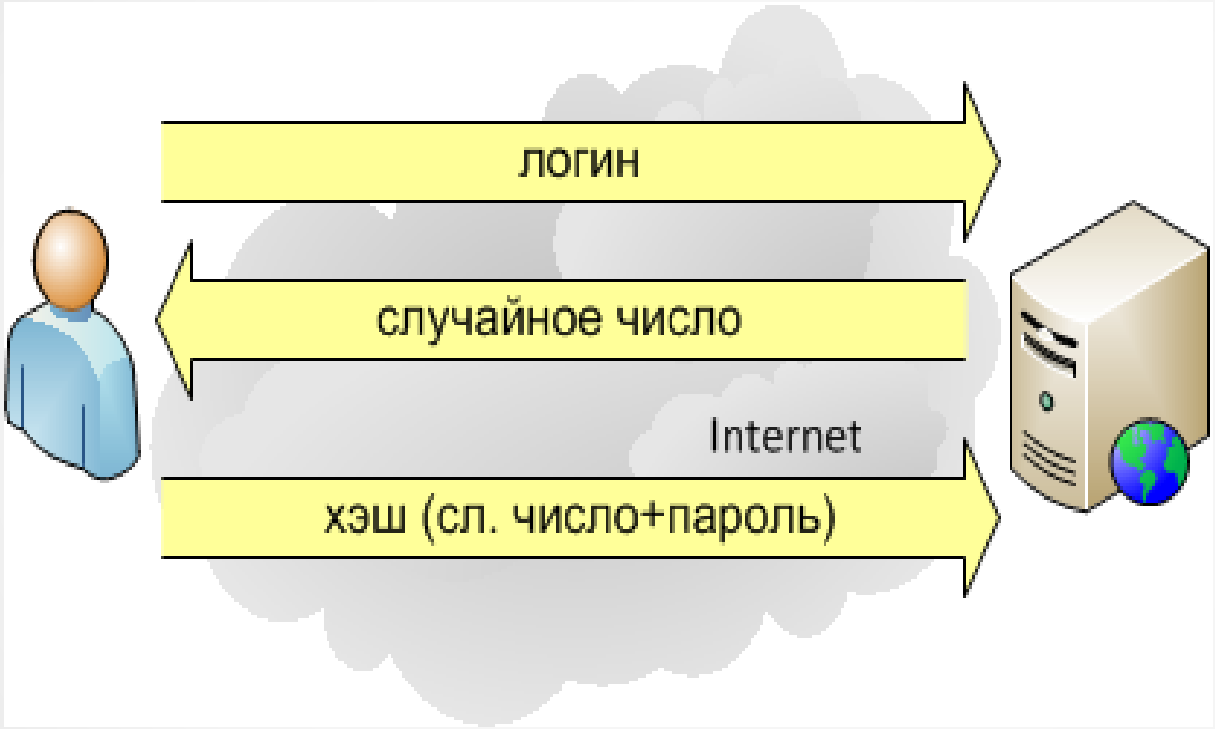
- подбор паролей
- просмотр паролей в системе
- перехват паролей при передачи
- пароль можно «подсмотреть» при вводе
- человеческий фактор – человек не может запомнить сложные пароли (записывает), диктует открытым способом (по телефону) и т.д.
- каждый раз нужно набирать на клавиатуре
- нужна предварительная регистрация пользователя в системе

Удаленная аутентификация PAP



SSL, TLS, TTLS

Удаленная аутентификация CHAP



Основной недостаток - необходимо хранить пароль на сервере

Удаленная аутентификация MS-CHAP

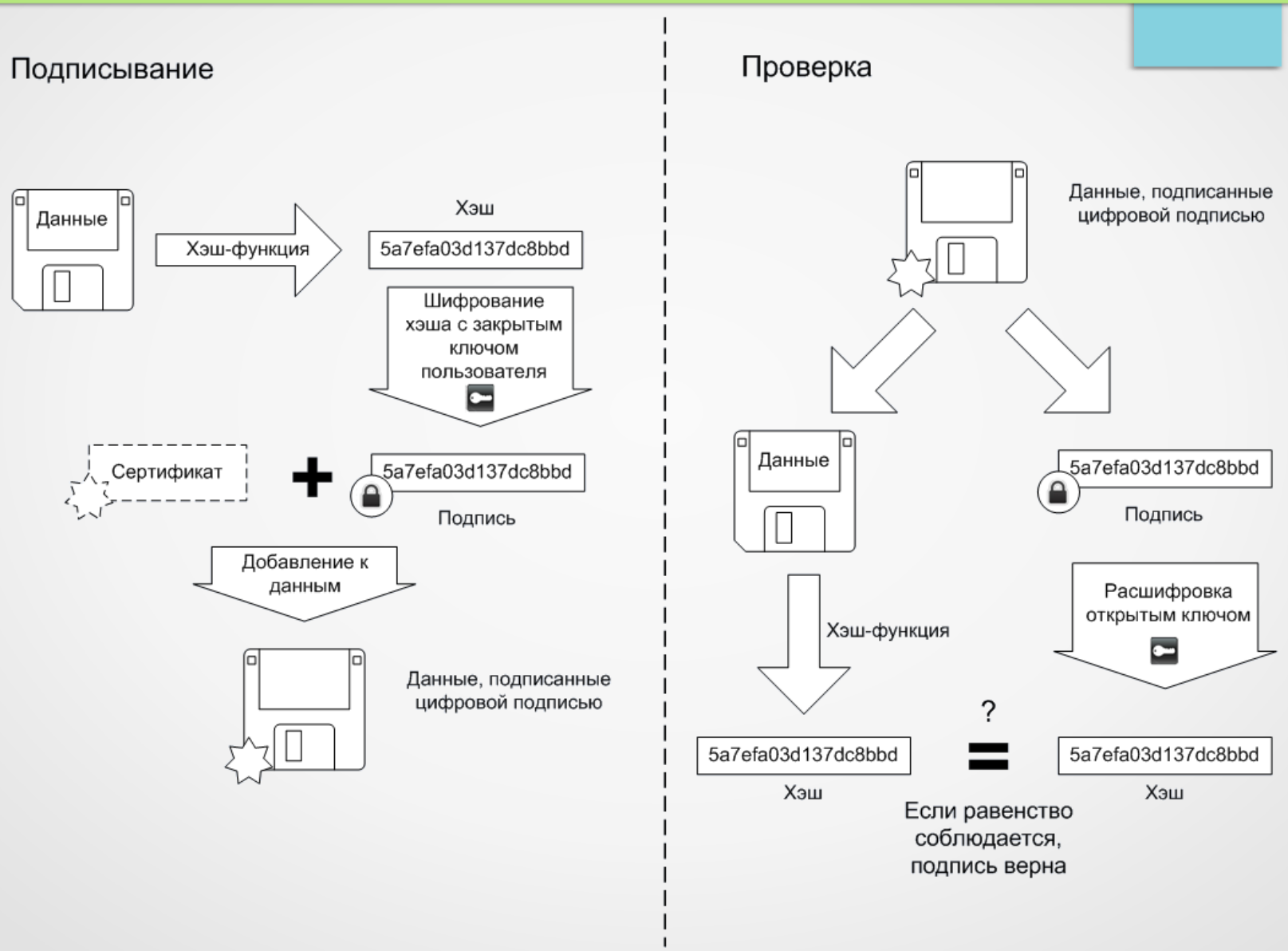
Аутентификация на базе ЭЦП

Построение безопасного механизма аутентификации при небезопасном соединении. Такой подход позволит аутентифицироваться на сервере, никогда не передавая серверу пароль, ни при регистрации, ни при аутентификации.

Регистрация
1 - Клиент выбирает login и password;
2 - На их основе формируется PrivateKey = SHA256(login+password);
3 - На основе PrivateKey формируется PublicKey;
4 - Login и PublicKey отправляются на сервер и сохраняются в БД.

Аутентификация
1 - Клиент вводит логин и пароль;
2 - На их основе формируется PrivateKey = SHA256(login+password);
3 - Клиент получает от сервера случайное число(RNDserver) и генерирует свое случайное число(RNDclient);
4 - С помощью PrivateKey клиент формирует ЭЦП Sign(SHA256(RNDserver+RNDclient)) и отправляет на сервер Login, RNDclient и ЭЦП;
5 - Сервер проверяет корректность ЭЦП с помощью PublicKey клиента, хранящегося в БД.

Аутентификация на базе ЭЦП



Идентификация и аутентификация с помощью ЭЦП

- Электронно-цифровая подпись может использоваться в качестве средства аутентификации, если она помещена на аппаратные средства типа интеллектуальной карты. Карта представляет серверу подписанный ЭЦП идентификатор или PIN пользователя, сервер проверяет электронно-цифровую подпись и тем самым проводит аутентификацию пользователя.
- Если пользователей очень много, то подпись пользователя должна содержать сертификат в соответствии со стандартом X.509, который использует цифровую подпись доверенного сертификационного центра. Сертификат имеет ограниченный срок действия, указанный в его содержании. Сертификаты могут распространяться по незащищенным каналам связи и храниться в памяти в незащищенном виде.
- ЭЦП как средство аутентификации любых цифровых данных.

Аутентификация информации

Существует несколько схем построения цифровой подписи:

На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.

На основе алгоритмов асимметричного шифрования. На данный момент такие схемы ЭП наиболее распространены и находят широкое применение.

Кроме этого, существуют другие разновидности цифровых подписей: групповая подпись, неоспоримая подпись, доверенная подпись. Их появление обусловлено разнообразием задач, решаемых с помощью ЭП. Например:

когда корреспонденты доверяют друг другу;

- выявление несанкционированный модифицированных (подмененных) сообщений во время передачи;
- выявление сфабрикованных во время передачи (фиктивных) сообщений;

когда корреспонденты не доверяют друг другу (не имеют оснований доверять).

- защита получателя от отказа отправителя от авторства (ренегатства со стороны отправителя)

Сертификат ЭЦП

Формат сертификата открытого ключа определен в рекомендациях Международного Союза по телекоммуникациям ITU (X.509) и документе RFC 3280 Certificate & CRL Profile организации инженерной поддержки Интернета Internet Engineering Task Force (IETF).

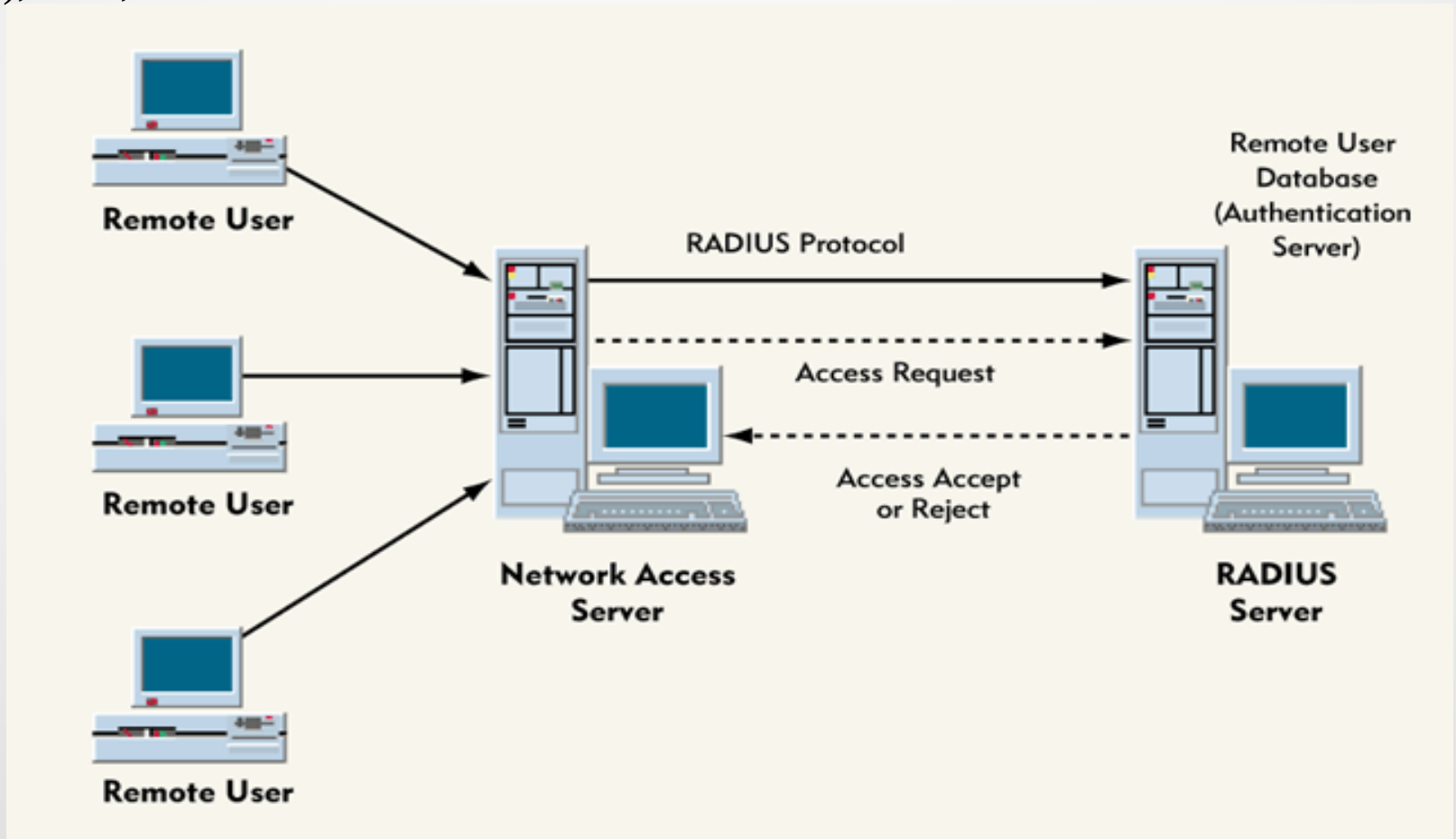
Сертификат открытого ключа подписи или шифрования представляет собой структурированную двоичную запись в формате абстрактной синтаксической нотации

Пример сертификата формата X.509

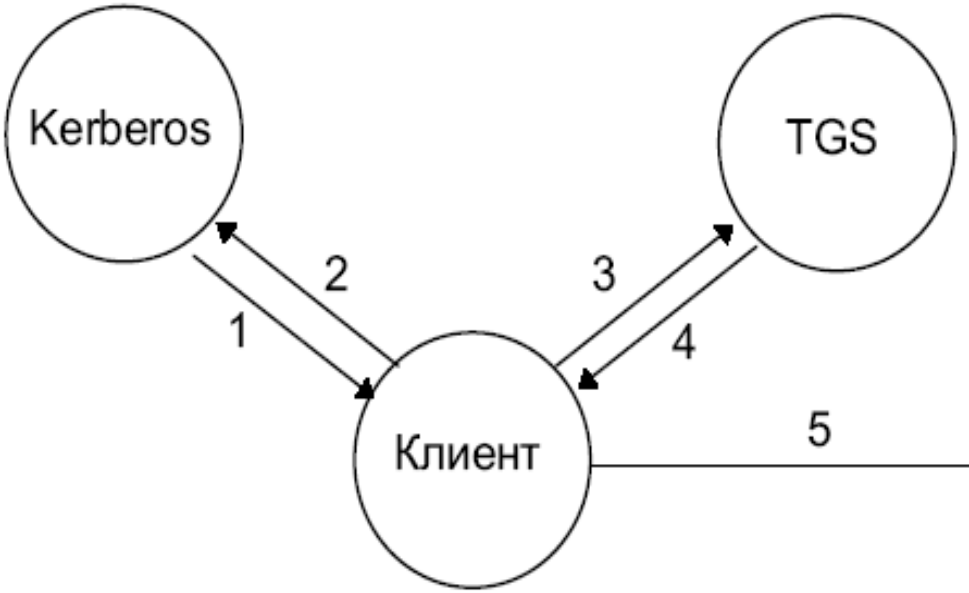
Имя пользователя: C = RU, org = ACME, cn = UserName
Имя издателя: C = RU, org = ACME
Номер сертификата: #12345678
Открытый ключ пользователя:
Алгоритм: GOST open key
Значение ключа: 010011101001001010000001
Сертификат действует с: 01.01.2006 00:00:00
Сертификат действует до: 31.12.2008 23:59:59
Дополнительная информация (X.509 v3 Extensions)
Регламент использования сертификата: Только для платежей
Секретный ключ действует с: 31.12.2006 23:59:59
Секретный ключ действует до: 31.12.2007 23:59:59
Область применения ключа: Идентификатор 1
Область применения ключа: Идентификатор i
Область применения ключа: Идентификатор N
Права и полномочия: Администратор
Атрибуты пользователя: IP, DNS, URI, RFC822, Номер счета, Адрес
...
Подпись Удостоверяющего Центра:
Алгоритм: GOST P 34.10-94 sign algorithm
Значение: 010011101001001010000001

Аутентификация в сети: Remote Authentication Dial-In User Service

«RADIUS RFC 2865 и RFC 2866 (Password Authentication Protocol, PAP), (Challenge Handshake Authentication Protocol, CHAP, MS-CHAP), (PPP, Point-to-Point Protocol), EAP, PPTP ...



Аутентификация в сети: Kerberos



1. Запрос мандата на выделение мандата
2. Мандат выделения мандата
3. Запрос мандата сервера
4. Мандат сервера
5. Запрос услуги

Аутентификация в сети: Kerberos